GrayAlpha Unmasked: New FIN7-Linked Infrastructure, PowerNet Loader, and Fake Update Attacks

By Insikt Group®

Archived: 2026-04-05 13:12:07 UTC

Executive Summary

Insikt Group identified new infrastructure associated with GrayAlpha, a threat actor that overlaps with the financially motivated group commonly referred to as FIN7. This newly identified infrastructure includes domains used for payload distribution and additional IP addresses believed to be tied to GrayAlpha. Insikt Group discovered a custom PowerShell loader named PowerNet, which decompresses and executes NetSupport RAT. Insikt Group identified another custom loader, referred to as MaskBat, that has similarities to FakeBat but is obfuscated and contains strings linked to GrayAlpha. Overall, Insikt Group found three primary infection methods: fake browser update pages, fake 7-Zip download sites, and the traffic distribution system (TDS) TAG-124. Notably, the use of TAG-124 had not been publicly documented prior to this report. Although all three infection vectors were observed being used simultaneously, only the fake 7-Zip download pages were still active at the time of writing, with newly registered domains appearing as recently as April 2025. Further analysis of these sites led to the identification of an individual who may be involved in the GrayAlpha operation.

In the near term, defenders are advised to enforce application allow-lists to block the download of seemingly legitimate files that contain malware. Where allow-lists are not practical, comprehensive employee security training becomes essential, particularly in recognizing suspicious behaviors such as unexpected prompts for browser updates or redirects caused by malvertising. Additionally, the use of detection rules, such as the YARA rules and Malware Intelligence Hunting queries provided in this report, is critical for identifying both existing and past infections. These rules should be updated frequently and supported with broader detection techniques, including monitoring of network artifacts and using Recorded Future Network Intelligence, due to the constantly evolving nature of malware.

Looking ahead, defenders must monitor the broader cybercriminal ecosystem to anticipate and respond to emerging threats more effectively. The continued professionalization of cybercrime increases the likelihood of organizations across multiple industries being targeted. This trend is driven by the sustained profitability of cybercrime, limited international law enforcement collaboration, and the continuous evolution of security technologies, which in turn drive innovation among threat actors. While advanced persistent threat (APT) activity is often linked to state-sponsored entities, GrayAlpha illustrates that cybercriminal groups can demonstrate a similar level of persistence. Much like the ransomware-as-a-service (RaaS) model, cybercriminals are becoming

increasingly specialized and collaborative, making it imperative to adopt a comprehensive and adaptive security posture.

Key Findings

- Insikt Group has identified new infrastructure linked to GrayAlpha — a threat actor overlapping with the group commonly known as FIN7 — including domains utilized for payload distribution and additional IP addresses believed to be part of the threat actor's infrastructure.
- Insikt Group has identified a new custom PowerShell loader dubbed PowerNet that decompresses and executes NetSupport RAT.
- Insikt Group identified another custom loader, referred to as MaskBat, which has similarities to FakeBat but is obfuscated and contains strings linked to GrayAlpha.
- Insikt Group identified three main infection vectors associated with GrayAlpha: fake browser update pages, fake 7-Zip download sites, and the TDS TAG-124 network. Notably, the use of the TDS TAG-124 delivery mechanism had not been publicly documented prior to this report.
- While all three infection methods were employed simultaneously, only the fake 7-Zip download pages appear to remain active at the time of writing, with the most recent domains surfacing as recently as April 2025.
- Through the analysis of the 7-Zip pages, Insikt Group identified an individual who may be connected to the GrayAlpha operation.

Background

GrayAlpha is a threat actor cluster that overlaps with the financially motivated cybercriminal group commonly known as FIN7, sharing key infrastructure, tooling, and tradecraft.

FIN7 has been active since at least 2013 and is considered one of the most prolific and technically sophisticated cybercriminal groups targeting organizations worldwide. The group is organized like a professional business, with compartmentalized teams handling malware development, phishing operations, money laundering, and management. FIN7 is primarily known for financially motivated campaigns involving the theft of payment card data and unauthorized access to corporate networks, particularly within the retail, hospitality, and financial sectors.

In 2018, the US Department of Justice (US DOJ) unsealed indictments against three high-ranking FIN7 members — Dmytro Fedorov, Fedir Hladyr, and Andrii Kolpakov — highlighting the group’s extensive operations against businesses across 47 US states and multiple countries. Operating under the name of a sham cybersecurity firm, “Combi Security,” FIN7 leveraged social engineering and customized malware, including variants of Carbanak, the group’s in-house developed backdoor, to compromise thousands of point-of-sale systems and exfiltrate over 15 million payment card records. The US DOJ prosecutions revealed the group’s hierarchical command structure, with members fulfilling defined roles in intrusion operations, malware administration, and logistical coordination. Despite the disruption to its leadership, FIN7’s underlying infrastructure and tradecraft persisted, enabling the broader criminal enterprise to continue targeting global organizations.

FIN7 uses a range of custom and repurposed malware and tooling to support its operations. The group typically gains initial access through spearphishing emails containing malicious attachments or links hosted on

compromised sites, often combined with callback phishing to increase credibility. FIN7's early operations leveraged its then-proprietary Carbanak backdoor as the primary command-and-control framework, enabling the group to manage compromised hosts and coordinate post-compromise activity. POWERTRASH — a uniquely obfuscated, PowerShell-based, in-memory loader adapted from the PowerSploit framework — has also been a consistent feature of FIN7 intrusions, used to deploy payloads such as DiceLoader and cracked Core Impact implants to support exploitation, lateral movement, and persistence. FIN7 also developed AuKill (also known as AvNeutralizer), a custom EDR evasion utility designed to disable endpoint security solutions, which was later reported to have been offered for sale by the group on criminal marketplaces. In its most recent campaigns, FIN7 has been observed deploying the Python-based Anubis backdoor, which provides full system control via in-memory execution and communicates with its command-and-control infrastructure using Base64-encoded data.

In 2023, FIN7 expanded its operations to include the deployment of ransomware through affiliations with RaaS groups such as REvil and Maze, while also managing its own RaaS programs, including the now-retired Darkside and BlackMatter. More recently, FIN7 has been observed leveraging NetSupport RAT embedded within malicious MSIX application packages, delivered via fake update sites and malvertising.

Threat Analysis

Infection Vectors

Over the past year, Insikt Group has identified three distinct infection vectors associated with GrayAlpha, observed during overlapping timeframes, and all ultimately resulting in NetSupport RAT infections. These vectors include:

- **Infection Vector 1:** Fake software updates impersonating legitimate products such as Concur
- **Infection Vector 2:** Malicious 7-Zip download pages
- **Infection Vector 3:** Use of the TAG-124 TDS

In these campaigns, GrayAlpha employed two primary types of PowerShell loaders: a self-contained custom script known as PowerNet, and a dynamic loader — a customized variant of FakeBat — referred to as MaskBat (see **Figure 1**).

Infection Vector 1: Fake Browser Updates

Infrastructure Analysis

Since at least April 2024, GrayAlpha has been observed leveraging fake browser update websites as part of its operations. These sites impersonate a range of legitimate products and services, including Google Meet, LexisNexis, Asana, AIMP, SAP Concur, CNN, the Wall Street Journal, and Advanced IP Scanner, among others. **Table 1** provides a list of domains associated with Infection Vector 1 that were still resolving as of 2025. However, it is important to note that active domain resolution does not necessarily indicate ongoing use by threat actors; in fact, the most recently observed domain began resolving in September 2024. A comprehensive list of all domains linked to Infection Vector 1 — including those that did not resolve at any point in 2025 — can be found in **Appendix A**.
